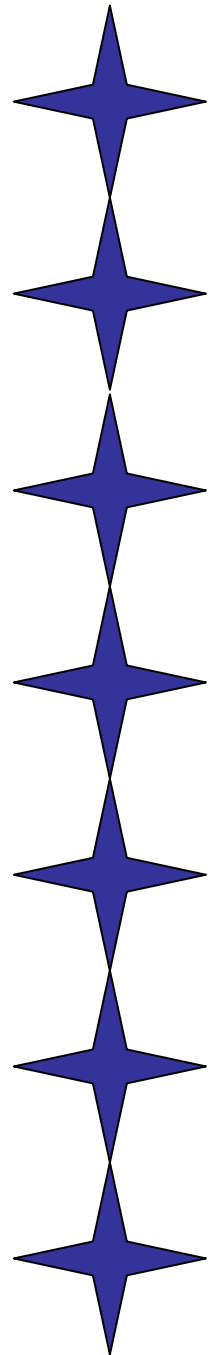


# CHSSTS Documentation

**Sophos Antivirus**

**James Schwar**

version 0.4  
Spring 2006



## Table of Contents

<b>1. Introduction.....</b>	<b>2</b>
1.1 Purpose of this document .....	2
1.2 Scope of this document .....	2
1.3 Reference .....	2
1.4 Overview of document .....	2
<b>2. General Description.....</b>	<b>2</b>
2.1 Product Functions.....	2
2.2 Similar System Information.....	2
2.3 User Characteristics.....	2
2.4 User Problem Statement.....	2
<b>3. Installing the Program.....</b>	<b>3</b>
3.1 Download the Installation Package .....	3
3.2 Run the Installer .....	3
3.3 Installation Package Install.....	3
3.4 Update the Program .....	4
3.5 Restart the Computer .....	5
<b>4. Configure and Run a Scan .....</b>	<b>5</b>
4.1 Open the Program.....	5
4.2 Configure a Full Scan .....	6
4.3 Scanning Options .....	7
4.4 Disinfection Options.....	8
4.5 Scan in Progress .....	9
4.6 Scan Completed.....	10
<b>5. Items in Quarantine.....</b>	<b>11</b>
5.1 Quarantine Manager .....	11
5.2 Move the File .....	11
5.3 Delete a File .....	12
<b>6. Things that Go Wrong.....</b>	<b>13</b>
6.1 Downloaded file Corrupted.....	13
6.2 Step 3.4 Update the Program Will not Work.....	13
6.3 New User Problems.....	13
6.4 Error 1325: Documents is not a Valid Short file Name.....	14

## **1. Introduction**

### **1.1 Purpose of this document**

This document is created with the intent that it will be used as a beginner's guide to detecting and removing viruses. It is hoped that this document will allow its readers to feel confident when using the virus scanner, and allow them to help themselves when professional support is not available, or not needed.

### **1.2 Scope of this document**

This document will cover the installation of the Sophos Antivirus program, along with its configuration and usage. It will provide visual and written descriptions of what to do and when to do it.

### **1.3 Reference**

<http://www.sophos.com>

## **2. General Description**

### **2.1 Product Functions**

Sophos has a simple and easy to use user interface and is a decent antivirus solution. Its ease of use for new users is nice. Plus the company allows the product to be installed on the home computers for free (an excellent decision). It lacks in configuration options for more advanced users, and also in reporting of viruses.

### **2.2 Similar System Information**

There are many different antivirus programs on the market and most are up to par. Norton, McAfee, and Trend Micro have three reputable products. All have different user interfaces and configuration options.

### **2.3 User Characteristics**

This document was written with the assumption that its reader could be anyone from the newest computer user to someone with advanced skills. The user

wishes to have an antivirus solution on the computer and wants a quick and easy way to get up and running.

### 3. Installing the Program

#### !!! WARNING !!!

Before performing any of the following steps make sure that you completely uninstall any other form of antivirus software that is on your computer. Not doing so can cause the installation package to fail, turning a relatively easy process into a horrible troubleshooting nightmare. Also, you must be an ADMINISTRATOR to complete these tasks.

#### 3.1 Download the Installation Package

If you are a faculty, staff, or student at Montclair State University you have the option to download Sophos Antivirus from the Office of Information Technology website. A direct link to the file is currently located at

[https://oit.montclair.edu/oit/dataio/win/Sophos\\_AutoUpdater\\_v5.exe](https://oit.montclair.edu/oit/dataio/win/Sophos_AutoUpdater_v5.exe)

You will be prompted for your netid and password, and after you entered this information the download should begin.

#### 3.2 Run the Installer

After the file has finished downloading an icon (as shown in figure 3.1) will be located somewhere on your system. You will need to “double-click” on the icon to begin the installation.



Figure 3.1

#### 3.3 Installation Package Install

Figure 3.2 illustrates the extraction and installation of the “Installation Package.” This program will extract the files that are needed to install Sophos Antivirus. It has been preconfigured to set up almost everything that you will need. Your only interaction for this process is to click on the button “Close” when the program finishes.

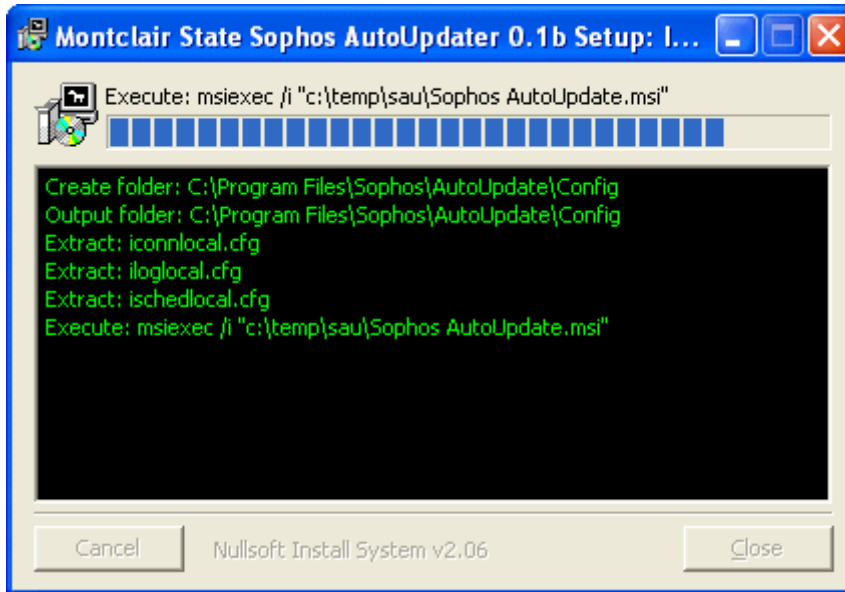


Figure 3.2

### 3.4 Update the Program

If the installation package has successfully installed you will see the “blue shield” in the bottom right hand corner of the screen. The “blue shield” is shown as the icon that is directly to the right of the “<” symbol in figure 3.3. You will need to “right click” on the icon to display the list of options. At the top of the list of options (also indicated in **bold**) is the “Update Now” option. You should select this as it will download all of the files needed and install them. Figure 3.4 illustrates what will be seen after selecting this option.



Figure 3.3



Figure 3.4

### 3.5 Restart the Computer

If everything has run successfully you will see what is depicted in figure 3.5. If you do not click on the “Close” button the computer will restart (make sure you choose “Close” if you have not saved your data). If you don’t wish to wait the 30 seconds then you can select the “Restart” button whenever you want.



Figure 3.5

## 4. Configuring and Run a Scan

### 4.1 Open the Program

There are several ways to open the Sophos Antivirus program, but the most common and easiest way is to “Right-Click” on the “Blue Shield” in the bottom right hand corner of the screen (as depicted in figure 3.3). You will know that the program has been opened if you see the interface that is shown in figure 4.1.

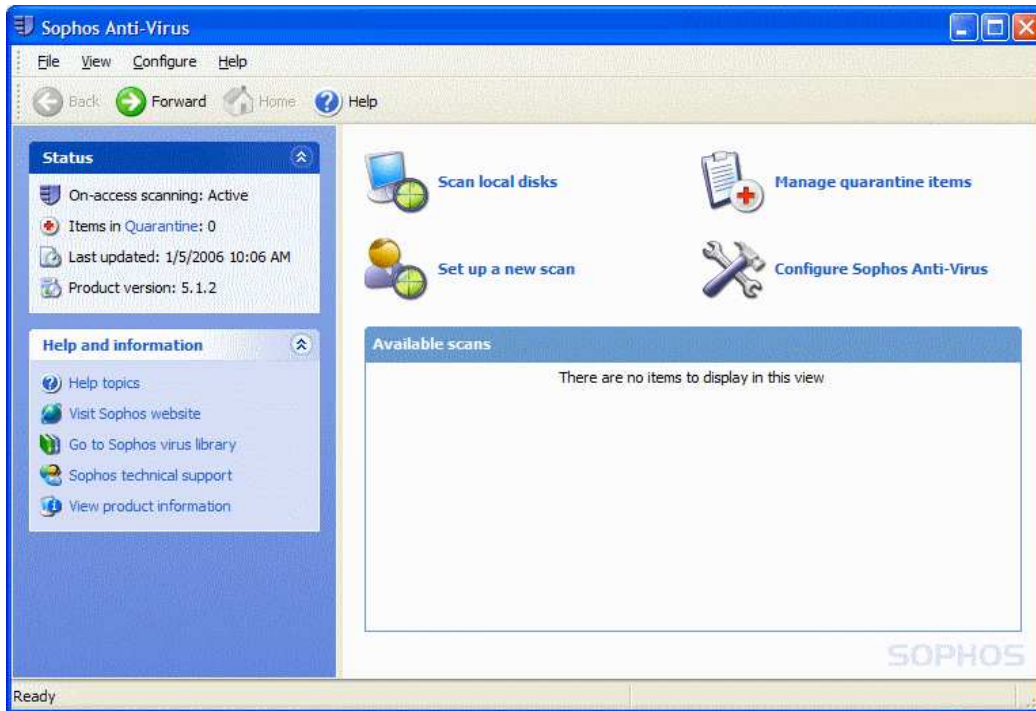


Figure 4.1

## 4.2 Configure a Full Scan

When you have opened the interface that is shown in Figure 4.1 you will probably want to configure a full system scan. I find that the options that are presented here will provide adequate protection for most users, but the options can always be modified to suit your needs. So we can begin by “Double-clicking” on the link for “Set up a new scan” as is shown in figure 4.1.

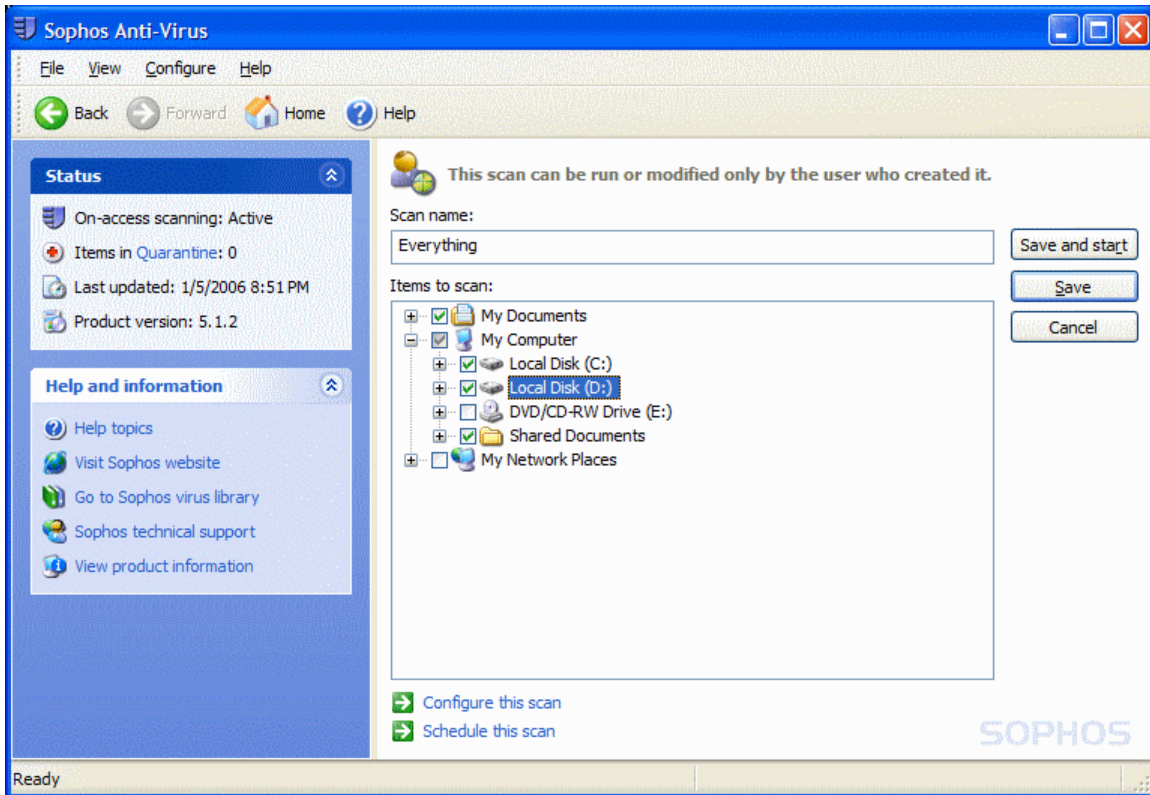


Figure 4.2

Figure 4.2 is the screen you will see after you have selected “Set up a new scan.” This is the area where you can set up what part(s) of the system you wish Sophos to scan. Begin first by giving this scan a name. I have chosen to name the scan “Everything” because with these settings every file that is located locally on the computer will be scanned for viruses. Then click on the boxes for the portion of the computer you would like to have scanned. If you are following the settings that are described here you can just click on the boxes for “Local Disk (C:)” and “Local Disk (D:).” The rest of the folders that are located under these two drives will automatically be selected.

### 4.3 Scanning Options

Now that you have selected what you would like to have scanned, you will want to configure how you want the scanning to proceed. Click on the link for “[→] Configure this Scan” that is located at the bottom of Figure 4.2 (it is colored blue). When you have clicked on the link the window that is shown in Figure 4.3 will be displayed on the screen. Make sure that the tab for “Scanning” at the top of the box is selected and choose the boxes that are shown.

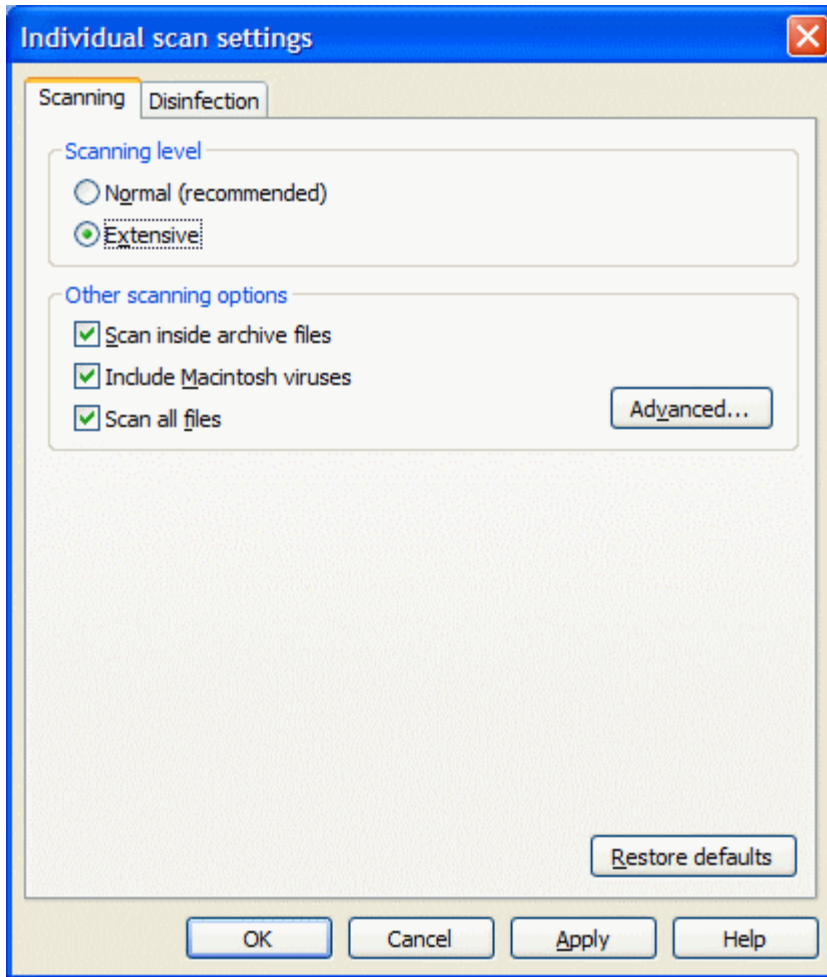


Figure 4.3

#### 4.4 Disinfection Options

With the same window open as shown in figure 4.3, choose the tab labeled “Disinfection.” (for a visual display of what is seen in the Disinfection tab please see figure 4.4) Here you will set what actions the program should take in the event that a virus is actually detected. Automatic disinfection is nice because it can remove the unwanted portions of program code from what are otherwise good programs. An example of where this could come in handy is: Let’s say that you have a Microsoft Word document that has become infected with a virus, and you want to keep the file and only get rid of the virus portions, this option will do just that. For “Other actions against infected files” choose “Do nothing.” This may sound counterintuitive but the “Do nothing” option actually moves the file(s) that has a virus into quarantine. While in quarantine the file is no longer a threat or a problem to your computer.

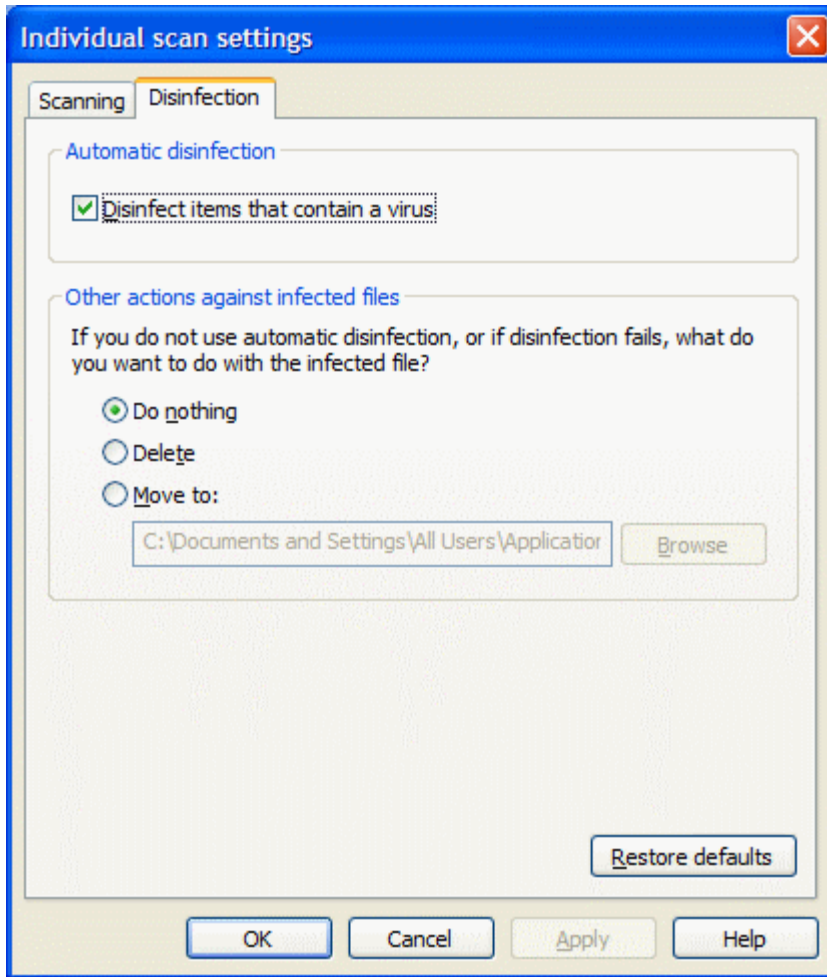


Figure 4.4

## 4.5 Scan in Progress

If you have not done so already you should click “Ok” on the box shown in Figure 4.4 and then click on “Save and start” as shown in figure 4.2. The scan will now run, this would be a good time for you to take a lunch, get some coffee, or anything you want, but please don’t sit and watch the progress waiting to see a virus pop up as this could take some time. If necessary you can stop or pause the scan if time does not permit you to wait for this task to finish. It is also possible to continue working on other projects while your computer is being scanned for viruses, but I don’t suggest this as the scanner is utilizing a large portion of processor space and it is continuously accessing the hard drive.

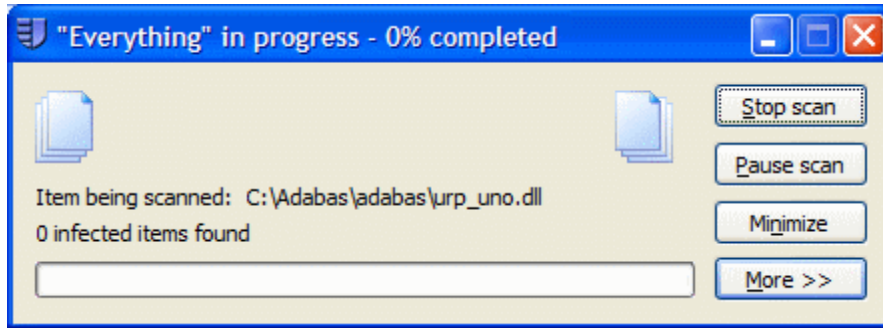


Figure 4.5

## 4.6 Scan Completed

When the scan has completed you should see the window as shown in Figure 4.6. You can click on the “More >>” button to see additional information about anything the scanner has deemed worthy to report about or you can click “Less <<” to not have to view this data. If any viruses were found you can click on the link in blue named “Quarantine.” This will allow you to manage what to do with the viruses. If no viruses were found or if you don’t wish to deal with them now you can always click on the button labeled “Close.”

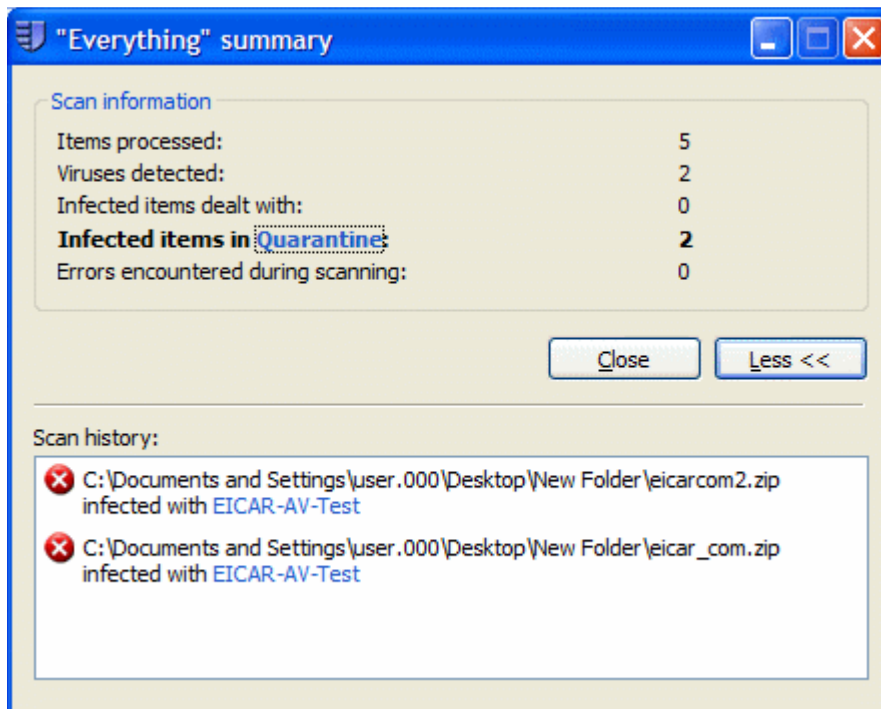


Figure 4.6

## 5. Items in Quarantine

### 5.1 Quarantine Manager

The Quarantine Manager (Figure 5.1) is the place where you can deal with items that are infected with viruses. Your options here are somewhat limited, but they are adequate when it comes to what a person would/should want to do with files infected with a virus. If you have not selected any of the files that are in your list of “items that need to be dealt with,” you will only be presented with two boxes that are clickable “Select all” and “Deselect all.” These options are self-explanatory. You can also select individual files by clicking on the boxes that are located under the “Item name” column.

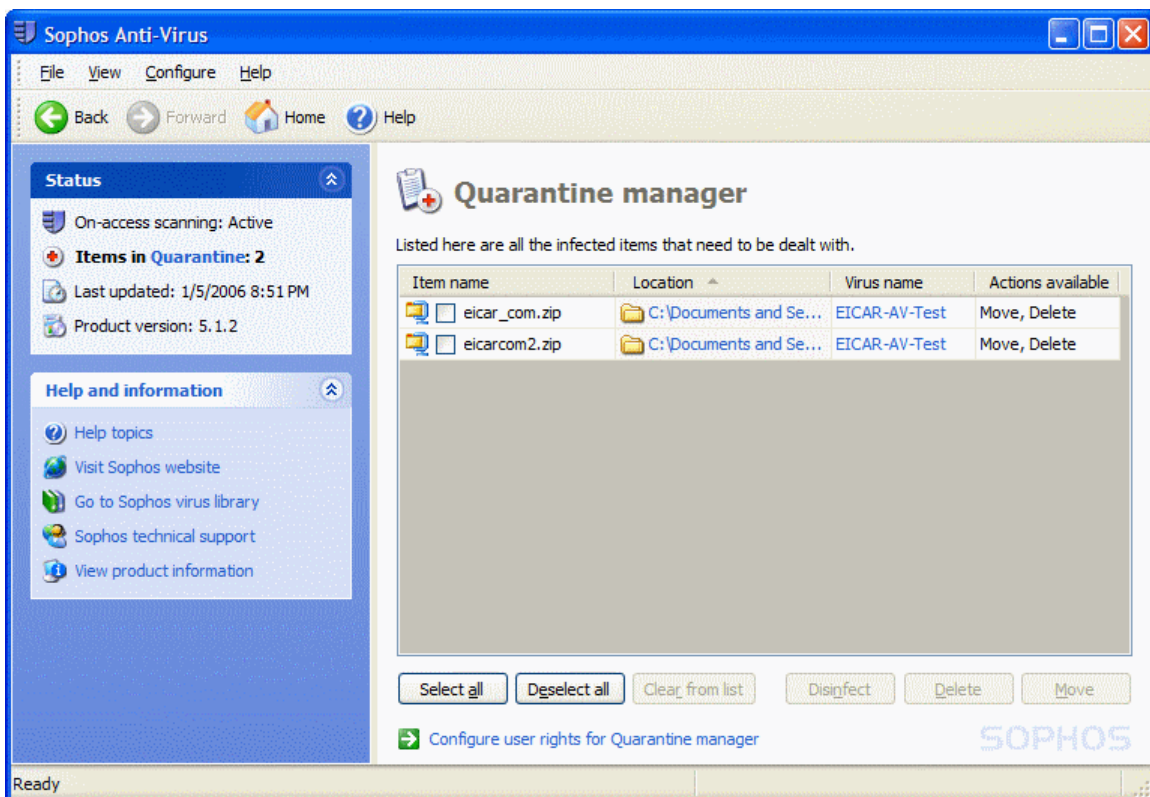


Figure 5.1

### 5.2 Move the File

Once you have selected a file or files that you wish to deal with there are only a handful of things you can do with them. If you wish to move the file, then you should only move the item to a form of removable media such as a flash drive or some other portable media. The logic behind this option is that you can get the infected file off of your machine and keep it around to attempt disinfection with another antivirus solution or you can hope for a later day when the Sophos package has the capability to disinfect the item. You will be prompted with a

window as the one shown in Figure 5.2 that will confirm that you really wish to take this action.

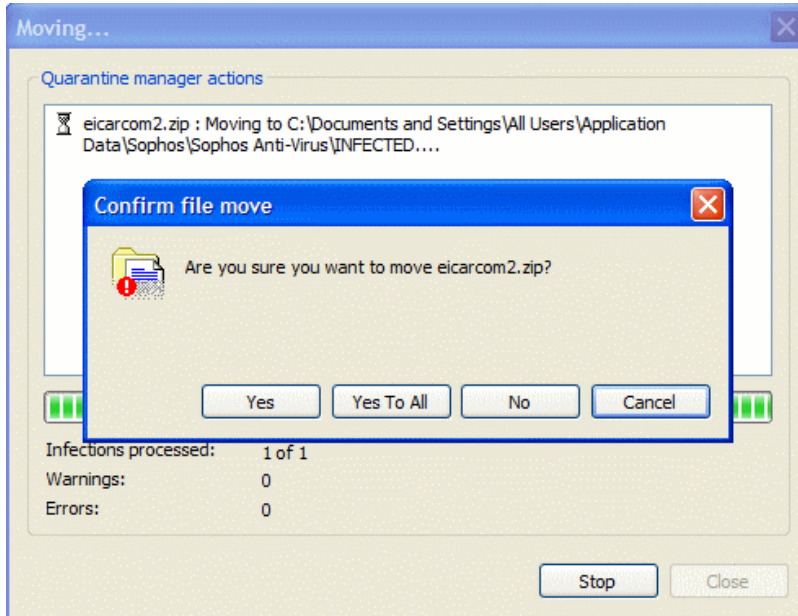


Figure 5.2

### 5.3 Delete a File

Deleting a file is a permanent action that means that you will never have access to this file again. It will ensure that you have removed the possibility that this particular copy of the virus can not affect your system again. However, it does not ensure that you will never be infected with the same virus again. As with the move option, you will be prompted to confirm that you really wish to remove this file from the computer. See Figure 5.3.

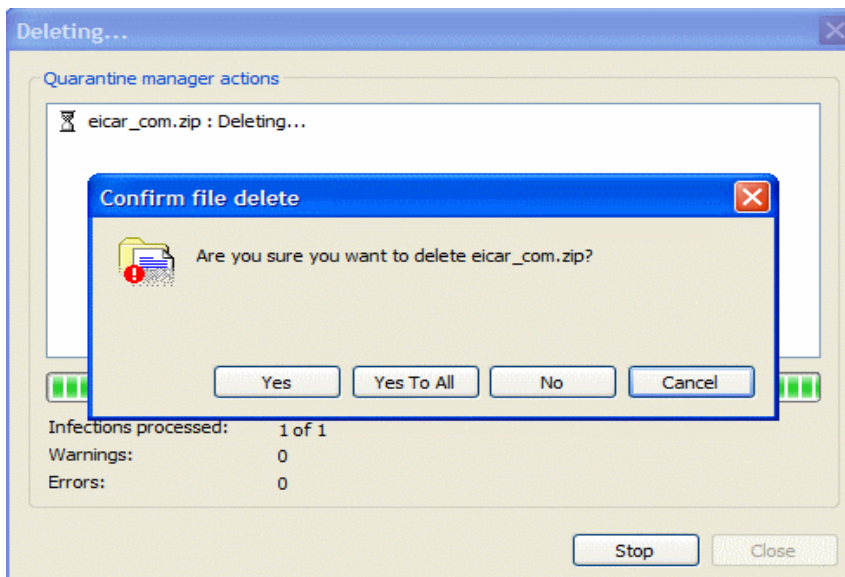


Figure 5.3

## 6. Things that Go Wrong

### 6.1 Downloaded File Corrupted

Occasionally the installation package will become corrupted (bad!) during the download. If this happens you will receive the “Error reading archive” message as is shown in Figure 6.1.



Figure 6.1

### 6.2 Step 3.4 Update the Program Will not Work

This is the step that actually installs the antivirus software and if it is not completed then you will not be protected from viruses. Most likely this occurred because you did not read the big bold WARNING that said to completely uninstall all previous versions of antivirus software. Another scenario is that some registry keys are lying around that are blocking the program from being installed.

Here is one known key that prevents the installer from working (others will be added when confirmed)

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\{87AEFD84-BC0D-11D4-B885-00508B022A51}
```

### 6.3 New User Problems

If you have added a new user to the system and this person can not run the Sophos Antivirus program then most likely they have not been added to any of the Sophos Groups and do not have the permissions to run the program. This can be remedied by logging onto the computer as an Administrator and by doing the following:

1. Go to Start → Run.
2. When the run box opens type in: `lusrmgr.msc`
3. Select the Groups pane, and add the user to one of the Sophos Groups.

## 6.4 Error 1325: Documents is not a Valid Short Filename

This error has been seen when Administrative user who is trying to install the file has an invalid address for their **My Documents** folder. You will most likely need to do the following to correct the error:

1. Go to Start and open the menu
2. *Right-click* on My Documents and select Properties
3. Click on the button labeled “Move...”
4. Select a valid location for the My Documents folder